



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/904,962	07/13/2001	Viswanath Ananth	5019P001X	7370

8791 7590 03/23/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER

KIM, JUNG W

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 03/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/904,962	ANANTH, VISWANATH	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 January 2005.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413). |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-20 have been examined. Applicant in the amendment filed on January 10, 2005 amended claims 1, 12, 17 and 18.

Response to Amendment

2. The objection to the specification is withdrawn as the amendment to the specification overcomes the objection.
3. The 112, second paragraph to claim 12 is withdrawn as the amendment overcomes the 112, second paragraph rejection.

Response to Arguments

4. The following is a response to the arguments presented by the applicants in the amendment filed on January 10, 2005.
5. Applicant's willingness to submit a terminal disclaimer to overcome the obviousness-type double patenting rejection when the claims as amended are in a condition for allowance is noted. In view of the amendments to the claims, a double patenting rejection is still warranted. Moreover, applicant is required to either cancel the conflicting claims from all but one application or maintain a clear line of demarcation between the applications. See MPEP § 822.

6. Applicant's arguments with respect to the 103(a) rejections of claims 1-20 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

7. Claims 18 and 20 are objected to because of the following informalities: claims 18 and 20 are not grammatical. Appropriate correction is required.

Double Patenting

8. Claims 12-14, and 17-19 of this application conflict with claims 1-8, 15-20, 22, 25 and 30-32 of copending Application No. 09,864,042. 37 CFR 1.78(b) provides that when two or more applications filed by the same applicant contain conflicting claims, elimination of such claims from all but one application may be required in the absence of good and sufficient reason for their retention during pendency in more than one application. Applicant is required to either cancel the conflicting claims from all but one application or maintain a clear line of demarcation between the applications. See MPEP § 822.

9. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225

Art Unit: 2132

USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

10. Claims 1-8, 12-14, and 17-19 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-8, 15-20, 22, 25 and 30-32 of copending Application No. 09,864,042. Although the conflicting claims are not identical, they are not patentably distinct from each other because both sets of claims define a cipher comprising a routine to divide incoming plain text into variable-sized blocks and a routine converting the plain text into cipher text based on an encryption key and an internal identifier. The additional limitation of an internal state affecting the conversion routine defined in the aforementioned claims of the instant application does not define a patentably distinct limitation since it is an inherent feature of a ciphering device.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

12. Claims 12-16 and 18 are rejected under 35 U.S.C. 102(e) as being anticipated by Barbir U.S. Patent No. 6,122,379 (hereinafter Barbir).

13. As per claims 12-16 and 18, Barbir discloses a computing device (figs. 3-8 and related text) comprising:

- a. a memory (fig. 3, reference no. 160); and
- b. logic coupled to the memory, the logic to perform a state-varying stream cipher operation, controlled by at least an encryption key and an internal state of

the computing device, on input data segmented in random sized blocks using an encryption key (col. 7:22-45);

c. wherein the stream cipher operation involves encryption (Abstract; 3:15-4:53);

d. wherein the logic is an integrated circuit (fig. 3, reference no. 140);

e. wherein the internal state of the computing device varies over time and wherein the variation of the internal state of the computing device is periodic being set at a time that an encryption process begins for each block of input data (fig. 4, especially reference nos. 40 and 98; fig. 6);

f. wherein the logic to segment the random sized blocks using the encryption key into a plurality of blocks including at least three successive blocks varying in length (fig. 4, reference no. 40; each new static stage size determines a successive block varying in length from previous block sizes).

14. The aforementioned cover the limitations of claims 12-16 and 18.

Claim Rejections - 35 USC § 103

15. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

16. Claims 1-3, 5, 6 and 9-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barbir in view of Zhang U.S. Patent No. 6,154,541 (hereinafter Zhang).

17. As per claims 1-3, 5, 6, 10 and 11, Barbir discloses a state-varying hybrid stream cipher operating within a computing device (figs. 3-8 and related text), comprising:

- g. a first software routine to divide incoming plain text into variable-sized blocks with each block varying in size (fig. 4, reference no. 40; each new static stage size determines a successive block varying in length from previous block sizes); and
- h. a second software routine to convert the plaintext into cipher text based on an encryption key and an internal state of the computing device (col. 7:22-45; fig. 5);
- i. wherein the first software routine produces the variable-sized blocks based on the encryption key (7:22-45);
- j. wherein each current block of the plain text is determined by producing a pseudo-random sequence using a second non-linear function including the encryption key as input and accessing contents of the pseudo-random sequence as a number of data elements of the plain text forming the current block (fig. 4, reference no. 40); and
- k. a fourth software routine further performs a first shuffling operation on an internal state of a computing device based on the encryption key so that a single bit modification of the encryption key requires complete recalculation of the internal state of the computing device (fig. 5);

- l. wherein the internal state of the computing device is periodically modified (fig. 6, reference no. 330);
 - m. wherein the internal state of the computing device is based on a time value (fig. 6; reference no. 330);
18. Barbir does not expressly disclose incorporating a unique internal identifier and an output of a first non-linear function along with the encryption key for the production of the random-sized blocks; incorporating the unique internal identifier as inputs to the second non-linear function to produce the pseudo-random sequence; wherein the second software routine further performs a second shuffling operation on the internal state of the computing device based on the encryption key and internal identifier to mitigate a likelihood of prediction of the internal state of the computing device upon knowledge of the encryption key. Zhang teaches incorporating efficient methods to secure a cipher system by multi-seeding and re-seeding, wherein multiple values, including an identifier from a source, are incorporated using a non-linear function combined with other seeds to establish a randomizing function. Zhang, 21:43-22:47, especially 22:19-36. It would be obvious to one of ordinary skill in the art at the time the invention was made for the hybrid stream operation processed by the logic to produce random-sized blocks of the input data based on the encryption key, an unique internal identifier and an output of a first non-linear function, wherein each block of the plain text is determined by the hybrid stream cipher producing a pseudo-random sequence using a second non-linear function including the encryption key, the internal identifier and the output of the first non-linear function as inputs; and wherein the second software routine

further performs a second shuffling operation on the internal state of the computing device based on at least the internal identifier to mitigate a likelihood of prediction of the internal state of the computing device upon knowledge of the encryption key, since multi-seeding and re-seeding and any combination thereof to generate functions of the cryptosystem enables a more secure cryptosystem. Zhang, 21:65-22:8. The aforementioned cover the limitations of claims 1-3, 5, 6, 10 and 11.

19. As per claim 9, the rejection to claim 1 under 35 U.S.C. 103(a) is incorporated herein. Although Barbir does not expressly teach a routine distributing error correcting codes in the cipher text in order to correct modifications, error correcting codes are well known features in the art of networking to identify and correct errors occurring to digital data during transmission. Some examples are: parity, checksums and CRC. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for a third software routine to distribute error correcting codes in the cipher text in order to identify and correct modifications as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 9. Note: the common knowledge or well-known statement in the rejection of claim 9 is taken to be admitted prior art. MPEP 2144.03.C ("If applicant does not traverse the examiner's assertion of official notice or applicant's traverse is not adequate, the examiner should clearly indicate in the next Office action that the common knowledge or well-known in the art statement is taken to be admitted prior art because applicant

Art Unit: 2132

either failed to traverse the examiner's assertion of official notice or that the traverse was inadequate")

20. Claims 4, 7, 8, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barbir in view of Zhang, and further in view of Moskowitz et al. U.S. Patent No. 5,822,432 (hereinafter Moskowitz).

21. As per claims 4 and 7, the rejections of claim 1-3, 5, 6 and 10 under 35 U.S.C. 103(a) are incorporated herein. Barbir does not disclose a third software routine to determined if a plurality of random data elements are to be distributed within the cipher text and to compute a hash digest of the random data elements, wherein the third software routine determines an amount of random data elements distributed within the cipher text is programmable based on a percentage value entered by a user. Moskowitz teaches a method of inserting random values into a digital stream, which are based on human interactive input information, by mapping these values into the digital stream wherein a pseudo-random key is used to identify the locations of the random values, wherein a hash digest of random data elements is computed. See Moskowitz, Abstract; Figure 1 and related text; col. 5:6-6:7; claims 1, 4 and 23-30. It would be obvious to one of ordinary skill in the art at the time the invention was made for the cipher to include a third software routine to determined if a plurality of random data elements are to be distributed within the cipher text and to compute a hash digest of the random data elements, wherein the third software routine determines an amount of

random data elements distributed within the cipher text is programmable based on a percentage value entered by a user, since it affords greater flexibility to a user of the system to adaptively change the parameters on the insertion of a watermark, thereby enabling the user to minimize the footprint while maximizing the security of the watermark. Moskowitz, 2:31-55. The aforementioned cover the limitations of claims 4 and 7.

22. As per claim 8, the rejections of claims 4 and 7 under 35 U.S.C. 103(a) is incorporated herein. Moskowitz discloses the distribution and amount of random data elements distributed within the cipher text is programmable based on a percentage entered by a user, but does not disclose that the distribution of random data elements distributed within the cipher text is based on the encryption key, the internal identifier and the internal state of the state-varying hybrid stream cipher. Zhang teaches multi-seeding and re-seeding techniques to generate a randomizing function for a cipher system. Zhang, col. 21:43-22:36. Moreover, the randomization function is deterministic to enable an inverse operation; hence, the output of the randomizing function is based on values corresponding to the known state of the cipher. As such, values such as the encryption key and the internal identifier are obvious seeds in combination with the internal state of the computing device to generate the amount of random data elements to be distributed within the cipher text. It would be obvious to one of ordinary skill in the art at the time the invention was made for the distribution of random data elements within the cipher text to be based on the encryption key, the internal identifier and the

internal state of the state-varying hybrid stream cipher. One would be motivated to do this to automatically distribute random but deterministic values as known to one of ordinary skill in the art. Zhang, *ibid.* The aforementioned cover the limitations of claim 8.

23. As per claims 19-20, the rejections of claims 1-11 under 35 U.S.C. 103(a) are incorporated herein. In addition, a corresponding decryption method is taught. See Barbir, col. 9:37-67; see Zhang, 21:54-55; see Moskowitz, 8:27-65, claims 1-10. The aforementioned cover the limitations of claims 19-20.

24. Claim 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barbir in view of Schneier Applied Cryptography (hereinafter Schneier).

25. As per claim 17, the rejection of claim 12 under 35 U.S.C. 102(e) is incorporated herein. Barbir does not expressly disclose the computing device is one of a smart card and an operating system. Schneier teaches incorporating cipher systems on a smart card, wherein the smart card is a portable storage medium, has an operating system and is tamper resistant. See Schneier, pg. 587, 'Smart Cards'. It would be obvious to one of ordinary skill in the art at the time the invention was made for the computing device to be one of a smart card an operating system, since smart cards affords a portable but secure means of housing the computing device as taught by Schneier, *ibid.* The aforementioned cover the limitations of claim 17.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

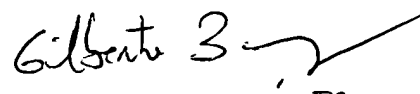
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jung W Kim
Examiner
Art Unit 2132

Jk
March 18, 2005



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100